AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Assistant Administrator for Procurement, Office of Procurement, NASA Headquarters (Code H).

[61 FR 40537, Aug. 5, 1996, as amended at 63 FR 9953, Feb. 27, 1998; 64 FR 19926, Apr. 23, 1999; 68 FR 23423, May 2, 2003; 70 FR 52941, Sept. 6, 2005]

PART 1803—IMPROPER BUSINESS PRACTICES AND PERSONAL CONFLICTS OF INTEREST

Subpart 1803.1—Safeguards

Subpart 1803.70—IG Hotline Posters

AUTHORITY: 42 U.S.C. 2473(c)(1)

SOURCE: 61 FR 40537, Aug. 5, 1996, unless otherwise noted.

Subpart 1803.1—Safeguards

1803.104 Procurement integrity.

1803.104–1 Definitions.

Agency ethics official means for Headquarters, the General Counsel and the Associate General Counsel for General Law, and for each center, the Chief Counsel.

[62 FR 36704, July 9, 1997. Redesignated at 67 FR 30603, May 7, 2002]

Subpart 1803.70—IG Hotline Posters

1803.7000 Policy.

NASA requires contractors to display NASA hotline posters prepared by the NASA Office of Inspector General on those contracts specified in 1803.7001, so that employees of the contractor having knowledge of waste, fraud, or abuse, can readily identify a means to contact NASA's IG.

[66 FR 29727, June 1, 2001]

1803.7001 Contract clause.

Contracting officers must insert the clause at 1852.203–70, Display of Inspector General Hotline Posters, in solicitations and contracts expected to exceed $5,000,000 and performed at contractor facilities in the United States.

[66 FR 29727, June 1, 2001]

PART 1804—ADMINISTRATIVE MATTERS

Subpart 1804.1—Contract Executive

Subpart 1804.4—Safeguarding Classified Information Within Industry

AUTHORITY: 42 U.S.C. 2473(c)(1).

SOURCE: 61 FR 40539, Aug. 5, 1996, unless otherwise noted.

Subpart 1804.1—Contract Execution

1804.170 Contract effective date.

(a) *Contract effective date* means the date agreed upon by the parties for beginning the period of performance under the contract. In no case shall the effective date precede the date on which the contracting officer or designated higher approval authority signs the document.

(b) Costs incurred before the contract effective date are unallowable unless they qualify as precontract costs (see FAR 31.205–32) and the clause prescribed at 1831.205–70 is used.

Subpart 1804.4—Safeguarding Classified Information Within Industry

1804.402 General.

(b) NASA security policies and procedures are prescribed in NPD 1600.2A, NASA Security Policy; NPR 1620.1, Security Procedural Requirements; NPR

2810.1 and NPD 2810.1 Security of Information Technology.

[66 FR 53546, Oct. 23, 2001, as amended at 69 FR 63459, Nov. 2, 2004]

1804.404–70 Contract clause.

The contracting officer shall insert the clause at 1852.204–75, Security Classification Requirements, in solicitations and contracts if work is to be performed will require security clearances. This clause may be modified to add instructions for obtaining security clearances and access to security areas that are applicable to the particular acquisition and installation.

1804.470 Security requirements for unclassified information technology resources.

1804.470–1 Scope.

This section implements NASA's acquisition-related aspects of Federal policies for assuring the security of unclassified automated information resources. Federal policies include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*), the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 *et seq.*), Public Law 106–398, section 1061, Government Information Security Reform, OMB Circular A–130, Management of Federal Information Resources, and the National Institute of Standards and Technology security guidance and standards.

[67 FR 48815, July 26, 2002]

1804.470–2 Policy.

(a) NASA policies and procedures on security for automated information technology are prescribed in NPD 2810.1, Security of Information Technology, and in NPR 2810.1, Security of Information Technology. The provision of information technology (IT) security in accordance with these policies and procedures, is required in all contracts that include IT resources or services in which a contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

(2) Acquisition, transmission or analysis of data owned by NASA with significant replacement costs should the contractor's copy be corrupted; and

(3) Access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The contractor must not use or redistribute any NASA information processed, stored, or transmitted by the contractor except as specified in the contract.

[66 FR 36491, July 12, 2001, as amended at 69 FR 63459, Nov. 2, 2004]

1804.470–3 Security plan for unclassified Federal Information Technology systems.

(a) The requiring activity with the concurrence of the Center Chief Information Officer (CIO), and the Center Information Technology (IT) Security Manager, must determine whether an IT Security Plan for unclassified information is required.

(b) IT security plans must demonstrate a thorough understanding of NPR 2810.1 and NPD 2810.1 and must include, as a minimum, the security measures and program safeguards planned to ensure that the information technology resources acquired and used by contractor and subcontractor personnel—

(1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards;

(5) Document and follow a virus protection program for all IT resources under its control; and

(6) Document and follow a network intrusion detection and prevention program for all IT resources under its control.

(c) The contractor must be required to develop and maintain an IT System Security Plan, in accordance with NPR 2810.1, for systems for which the contractor has primary operational responsibility on behalf of NASA.

(d) The contracting officer must obtain the concurrence of the Center Chief of Security before granting any contractor requests for waiver of the screening requirement contained in the clause at 1852.204–76.

[66 FR 36491, July 12, 2001, as amended at 69 FR 63459, Nov. 2, 2004]

1804.470–4 Contract clauses.

The contracting officer must insert a clause substantially the same as the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts which require submission of an IT Security Plan.

[66 FR 36491, July 12, 2001]